Claims

1. A computer system for adding two or more integers, comprising:

a memory unit operable to store a program composed of a plurality of instructions; and

a processor operable to fetch each instruction in turn from the program stored in the memory unit, and decode and execute each fetched instruction, wherein

the program includes

a conversion instruction set to have the processor generate elements belonging to a group G by implementing a power operation in the group G using each integer,

an operation instruction set to have the processor generate an operation value by implementing a basic operation other than addition using all the generated elements, and

an inverse conversion instruction set to have the processor generate a sum value of the integers by implementing, in the group G or a proper subgroup S of the group G, an inverse power operation on the operation value.

2. The computer system of Claim 1 securely and reliably manipulating target information, wherein

the program further includes a security instruction set to have the processor implement security processing on the target information, and

the security instruction set has the processor implement an addition operation using the conversion instruction set, the operation instruction set, and the inverse conversion instruction set.

3. The computer system of Claim 2, wherein

the group G is a multiplicative group of an integer residue ring,

the conversion instruction set has the processor implement an exponentiation to each of the integers, and

the operation instruction set has the processor implement a multiplication of the elements.

4. The computer system of Claim 3, wherein

the group G is a multiplicative group of Z/nZ where a product $n = p_1 \times p_2 \times \dots \times p_k$, and where $p_1, p_2, \dots, p_k$ ($k>1$) denote mutually differing primes, and

an operator $\times$ denotes multiplication, Z denotes an integer ring, and Z/nZ denotes an integer residue ring composed of values that are congruent modulo m.

5. The computer system of Claim 4, wherein

the inverse conversion instruction set includes instructions to have the processor solve a discrete logarithm problem in each of the multiplicative groups of $Z/Zp_1, Z/Zp_2, \dots, Z/Zp_k$, which use the primes $p_1, p_2, \dots, p_k$, respectively.

6. The computer system of Claim 5, wherein

the inverse conversion instruction set includes instructions to have the processor use a Chinese Remainder Theorem to solve a discrete logarithm problem in each of the multiplicative groups of $Z/Zp_1, Z/Zp_2, \dots, Z/Zp_k$, which use the primes $p_1, p_2, \dots, p_k$, respectively.

7. The computer system of Claim 2, wherein

the group G is a multiplicative group of Z/nZ for which $n = p^m \times q$, where p and q are primes and m is a positive integer,

the conversion instruction set has the processor implement exponentiations to each of the integers, and

the operation instruction set has the processor implement a multiplication of the elements.

8. The computer system of Claim 7, wherein

the subgroup S is a multiplicative group of Z/p^mZ.

9. The computer system of Claim 7, wherein

the positive integer m is 2.

10. The computer system of Claim 2, wherein

the subgroup S is an anomalous elliptic curve group,

the conversion instruction set has the processor implement a multiplication on the elliptic curve using each integer,

and the operation instruction set has the processor implement an addition of the elements on the elliptic curve.

11. The computer system of Claim 2, wherein

the group G is a direct product of two anomalous elliptic curve groups,

the conversion instruction set has the processor implement a multiplication on the elliptic curve using each integer, and

the operation instruction set has the processor implement an

addition of the generated elements on the elliptic curve.

12. The computer system of Claim 2, wherein

the inverse conversion instruction set has the processor store a plurality of exponents each in correspondence with a value raised to a power using a respective exponent, and find the inverse of the power operation by searching the correspondences.

13. The computer system of Claim 2, wherein

the inverse conversion instruction set includes a reduction portion to have the processor reduce each element belonging to the group G to an element belonging to the subgroup S.

14. The computer system of Claim 2 encrypting or decrypting the target information based on key information, wherein

the security instruction set has the processor encrypt or decrypt the target information based on the key information, the encryption and decryption being performed using the addition operation to add the key information or second key information obtained from the key information, to the target information or to second target information obtained from the target information, and

in the addition operation, the conversion instruction set, the operation instruction set, and the inverse conversion instruction set are used to add the key information or the second key information, to the target information or the second target information.

15. The computer system of Claim 14, wherein

the encryption is a shared key encryption algorithm, and the

decryption is a shared key decryption algorithm.

16. The computer system of Claim 2 implementing a digital signature or digital signature verification on the target information based on key information, wherein

the security instruction set implements the digital signature or digital signature verification on the target information based on the key information, making use of the addition operation to add the key information or second key information obtained from the key information to the target information or to second target information obtained from the target information, and

in the addition operation, the conversion instruction set, the operation instruction set and the inverse conversion instruction set are used to add the key information or to the second key information to the target information or the second target information.

17. The computer system of Claim 2, wherein

the processor and the memory are integrated on an IC card.

18. An addition method used for adding two or more integers using a computer system that includes a memory unit and a processor, the addition method comprising steps of:

a conversion step to cause the processor to generate elements belonging to a group G by implementing a power operation in the group G using each integer,

an operation step to cause the processor to generate an operation value by implementing a basic operation other than addition using all the generated elements, and

an inverse conversion step to cause the processor to generate a sum value of the integers by implementing, in the group G or a proper subgroup S of the group G, an inverse power operation on the operation value.

19. A computer program for adding two or more integers, the program, including:

a conversion instruction set for generating elements belonging to a group G by implementing a power operation in the group G using each integer,

an operation instruction set for generating an operation value by implementing a basic operation other than addition using all the generated elements, and

an inverse conversion instruction set for generating a sum value of the integers by implementing, in the group G or a proper subgroup S of the group G, an inverse power operation on the operation value.

20. The program of Claim 19, wherein

the program is recorded on a computer readable recording medium.

21. The program of Claim 19,

wherein the program is transmitted on a carrier wave.

22. A computer readable recording medium having a program for adding two or more integers recorded thereon, wherein

the program includes:

a conversion instruction set for generating elements belonging

to a group G by implementing a power operation in the group G using each integer,

an operation instruction set for generating an operation value by implementing a basic operation other than addition using all the generated elements, and

an inverse conversion instruction set for generating a sum value of the integers by implementing, in the group G or a proper subgroup S of the group G, an inverse power operation on the operation value.